Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Sunday, August 24, 2008

Smart contracts expand credit opportunities

Way back in 1994 I wrote the following (the "keys" here were envisioned as digital codes acting as car keys):

> If a loan was taken out to buy that car, and the owner failed to make payments, the smart contract could automatically invoke a lien, which returns control of the car keys to the bank. This smart lien might be much cheaper and more effective than a repo man.

I've since used this as one of the key examples of smart contracts, in particular smart contracts that help enforce security interests (collateral). Other kinds of smart contracts include digital rights management (for copyright licenses), financial cryptography (for payment systems and other kinds of financial contracts), price-sensitive controllers, and a wide variety of other possibilities. More recently, some real-world examples of the "auto-repo-auto" have appeared, and it is now becoming more common. Deborah Yao describes some more of these:

> Starter-interrupt devices are becoming a popular way for lenders to ensure they get paid, and consumers seem willing to accept them to get into nicer cars, use a smaller down payment and qualify for a lower interest rate, according to device manufacturers.
>
> ...The companies make a variation of the same device: The units are connected to the starter and emit a brief series of sounds or flashes of light, days before the payment deadline. If the customer then makes a timely payment, he or she can contact the dealer for a new code that will allow them to operate the vehicle. Some devices are remotely controlled by dealers.

Note that the process is far more manual and that there is much more attention to the user interface than I was thinking about in 1994. It's becoming increasingly apparent that a good user interface is often key to good security (phishing is another big example of this). Contracts are ultimately relationships between people, so a smart contract protocol needs to go all the way from end to end -- from person to person. Furthermore, as long as the parties have access to a good legal system, making certain important steps manual is a good idea if it increases flexibility and safety without too substantially decreasing security or user friendliness.

My thanks to Ian Grigg for pointing me to Yao's article.

Posted by Nick Szabo at 2:54 PM

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

2 comments:

Anonymous said...

I'm not some sort of economic Ted Kaczynski, but I worry about the secondary effects of lessening the 'arms-length' of credit transactions this way. Creditor's Rights is always a tricky body of law and experience for society to delineate, but I think this would eventually come to be seen as un-balanced in favor of the party with the technological leverage, (usually the creditor. . .)

Until I have the username and password for the creditor's bank account, I'm not going to feel comfortable giving him the kill-codes to my automobile (or 'key-codes' to my home. . .) I'm even more worried that, in pursuit of credit, other people *would*!

4:39 AM

nick said...

Anonymous, your concerns are well-placed, which as I take it are (1) resolving disputes between different creditors with security interests in the car, and (2) ensuring that the creditor does not abuse its power to remotely lock the ignition.

The biggest concern with the first problem is that this smart lien might be used as a secret lien, i.e. a lien other creditors cannot readily discover by searching the public financing statements, because the smart lien creditor can rely on the technology rather than the law to take control of the car. So the debtor might induce creditors to make further loans using the car as security but not knowing of the first smart and secret lien.

The general answer to the first concern is to align the protocols to secured transaction law more than my original proposal or the real-world implementations so far do. For example, instead of the conditional repo "keys" being held by the creditor or his agent, they could be held by a neutral third party that may also act as an arbitrator implementing the legal priority of the creditors, and can act as an agent of a state court(in the U.S.) or bankruptcy court for same. In this sense the protocol becomes a "smart remedy", in particular a smart distraint, which can be implemented automatically upon the verdict of the arbitrator or court. The first *publicly registered* lienholder (in the jargon of secured transaction law, the first perfected creditor) holds the physical power of repossession, but the arbitrator or court also holds the power to reverse this and give control to another creditor if the law should so imply.

To assist in this, the current system of public financing statements (that record the security interests of various creditors, so that other creditors are put on notice of these conditional rights) might be supplemented or replaced with a secure distributed database of security interests, implemented in the same way as secure property titles. When the control transfer conditions occurs (e.g. missing too many payments), the smart lien could automatically look at the database to determine the proper creditor to which to give control. Alternatively, it might be possible to automate the lookup and interpretation of current state financing statement databases to the same effect.

The answer to your second concern is not Mutual Assured Destruction (giving debtors the password to their creditors' bank account), but assuring that the *condition itself* is secure -- in other words, that the creditor physically cannot take control of the car unless the debtor really has not paid, and has loses all possibility of controlling the car in any way after said debtor has paid in full.

In this sense my original proposal solves (or at least plans to solve) this second problem, but the real-world implementations so far don't, and do indeed put more power than is ideal into the hands of creditors. Of course, debtors are free to decline to buy cars on credit using these mechanisms, but a fairer protocol, i.e. one in which the conditional logic is secure from both creditor and debtor, would be even better: more people would be willing to buy the cars, expanding credit opportunities.

1:51 PM

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ▼ 2008 (55)
  - ► December (2)
  - ► October (2)
  - ► September (4)
  - ▼ August (9)
    - Antiques, time, gold, and bit gold
    - Flying money: a brief overview
    - Smart contracts expand credit opportunities
    - Wet code and dry
    - Genoa
    - Patterns of integrity
    - Reruns
    - Inflation expectations, gold, and oil
    - Bank notes from the free banking era
  - ► July (4)
  - ► June (6)
  - ► May (6)
  - ► April (4)
  - ► March (10)
  - ► February (5)
  - ► January (3)
- ► 2007 (47)
- ► 2006 (130)

Post a Comment

► 2005 (44)

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.